613-001767 Rev.B 130515

最初にお読みください

CentreCOM® x510シリーズ リリースノート

この度は、CentreCOM x510 シリーズをお買いあげいただき、誠にありがとうございます。このリリースノートは、取扱説明書、コマンドリファレンス、VCS 設定 / 運用マニュアルの補足や、ご使用の前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1 ファームウェアバージョン 5.4.3-0.1

2 本バージョンで追加・拡張された機能

ファームウェアバージョン **5.4.2A-0.1** から **5.4.3-0.1** へのバージョンアップにおいて、以下の機能が追加・拡張されました。

2.1 1000BASE-T SFP モジュール AT-MG8T

1000BASE-T SFP モジュール AT-MG8T をサポートしました。

2.2 1000Mbps（LC）SFP モジュール AT-SPBD40-13/I、AT-SPBD40-14/I

一心双方向 1000Mbps SFP モジュール AT-SPBD40-13/I と AT-SPBD40-14/I をサポートしました。
AT-SPBD40-13/I と AT-SPBD40-14/I は対向で使用する必要があります。

2.3 findme コマンド

参照「コマンドリファレンス」/「運用・管理」/「システム」

機器のポート LED を一定期間（デフォルト 60 秒間）点滅させる findme コマンドが追加されました。このコマンドは、ラック内で機器の位置を確認したいときなどに便利です。

2.4 省電力イーサネット（Energy Efficient Ethernet）

参照「コマンドリファレンス」/「運用・管理」/「システム」

IEEE 802.3az 省電力イーサネット（Energy Efficient Ethernet）をサポートしました。
100BASE-TX/1000BASE-T ポートの非通信時の状態を制御し、消費電力を抑えることができます。

2.5 Syslog メッセージのバッファ設定コマンドの追加

参照「コマンドリファレンス」/「運用・管理」/「ログ」

ログを Syslog サーバーに送る前に一時的にバッファする log host startup-delay コマンドを追加しました。
ログ送信までの時間は log host startup-delay delay コマンドで、バッファするログメッセージ数は log host startup-delay message コマンドで設定します。

2.6 MAC アドレススラッシングプロテクショントラップ

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

MAC アドレススラッシングを検出した際、SNMP マネージャーに TRAP を送信する MAC アドレススラッシングプロテクショントラップをサポートしました。snmp-server enable trap コマンドで指定できる通知メッセージ種別に thrash-limit が追加されました。

2.7 トラップ送信タイミングの設定コマンドの追加

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ 起動時に送信する SNMP トラップの送信タイミングを設定する snmp-server startup-trap-delay コマンドを追加しました。

○ 対象インターフェースのリンクステータスが変化した時に送信する SNMP トラップの送信タイミングを設定する snmp trap link-status trap-delay コマンドを追加しました。

2.8 NTP の IP インターフェース設定

参照「コマンドリファレンス」/「運用・管理」/「NTP」

NTP の通信を行うインターフェースを指定する機能をサポートしました。インターフェースは ntp source コマンドで設定します。

2.9 ARP のマルチキャスト MAC アドレス対応

参照「コマンドリファレンス」/「IP ルーティング」/「ARP」

マルチキャスト MAC アドレスを含んだ ARP パケットを受信可能にする arp-mac-disparity コマンドをサポートしました。
これにより、Microsoft Network Load Balancing（MS-NLB）などのマルチキャスト MAC アドレスを用いて動作するサービスに対応します。

2.10 L3 テーブルのハッシュキー生成アルゴリズム

参照「コマンドリファレンス」/「IP ルーティング」/「ARP」

L3 テーブルのハッシュキーを生成するアルゴリズムを変更する platform l3-hashing-algorithm コマンドが追加されました。L3 テーブルが飽和してネクストホップを追加することができない時は、本コマンドによりアルゴリズムを変更することで回避することができる場合があります。

2.11 VRRPv3

参照「コマンドリファレンス」/「IP ルーティング」/「VRRP」

IPv4/IPv6 ネットワーク向けの VRRP（Virtual Router Redundancy Protocol）である、VRRPv3 をサポートしました。これに合わせて、VRRP-MIB（RFC2787）のサポートが廃止され、VRRPv3-MIB（RFC6527）をサポートします。
また、VRRPv3 とともに、VRRPv3 Accept Mode をサポートします。これにより、ICMP パケットへの応答を含め、バーチャル IP アドレス宛の通信に対応することができます。なお、Accept Mode は常に有効であり、無効にすることはできません。

VRRPv3 は、ファームウェアバージョン **5.4.2A-0.1** で使用されている VRRPv2 とは互換性がありません。VRRPv2 と VRRPv3 を接続するためには、VRRPv3 をサポートする機器側でトランジションモードを有効にする必要があります。トランジションモードの有効 / 無効の設定は、transition-mode コマンドで行います。トランジションモードはデフォルトで無効です。トランジションモードによる VRRPv2 と VRRPv3 の混在は、ファームウェアバージョンアップなど、一時的に VRRPv2 機器と接続する必要がある場合のみ使用し、継続的な運用にはトランジションモードは使用しないでください。

ファームウェアバージョン **5.4.2A-0.1**（VRRPv2）から **5.4.3-0.1**（VRRPv3）への移行の際は、基本的に 1 台ずつネットワークから切り離して、ファームウェアをバージョンアップして、再び接続するという手順になります。この場合、通信の切断時間が長くなります。
以下の手順では、通信の切断時間を短く抑えることができ、また、VRRP マスタールーター側からのリモート接続のみでバージョンアップ作業を行うことができます。

1. VRRP マスタールーターとして運用している機器（以下、機器 A と呼びます）で、運用中の全てのバーチャルルーターの動作を無効にして、設定を保存します。
   VRRP マスタールーターとしての動作は、バックアップルーターとして運用されていた機器（機器 B と呼びます）に引き継がれます。
2. 機器 A のファームウェアをバージョンアップし、再起動します。
3. 機器 A に再度ログインし、運用中の全てのバーチャルルーターのトランジションモードを有効にします。
4. 機器 A で、運用中の全てのバーチャルルーターを有効にします。
5. VRRP マスタールーターとして動作している機器 B にリモートログインし、運用中の全てのバーチャルルーターの動作を無効にして、設定を保存します。
   VRRP マスタールーターとしての動作は、機器 A に再び引き継がれます。
6. 機器 B のファームウェアをバージョンアップし、再起動します。
7. 機器 B に再度ログインし、運用中の全てのバーチャルルーターを有効にします。
8. 機器 A で運用中の全てのバーチャルルーターのトランジションモードを無効にします。

VRRP を運用時のバージョンアップ手順は以上です。

2.12 MLD

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD」

MLD（Multicast Listener Discovery）をサポートします。
MLD は、LAN 上の IPv6 ルーターが IPv6 ノードとメッセージを交換し合い、LAN 上にどのマルチキャストグループの受信希望者（メンバー）がいるかを把握するためのプロトコルです。MLD は、IPv4 における IGMP（Internet Group Management Protocol）と同等の機能です。対応 MLD バージョンは MLDv1 と MLDv2 です。

2.13 DHCPv6

参照 「コマンドリファレンス」/「IP 付加機能」/「DHCPv6 サーバー」

IPv6 アドレスや設定情報を動的に提供または取得する、DHCPv6 サーバー機能、DHCPv6 クライアント機能をサポートしました。いずれも、IPv6 プレフィックスを割り当てる、DHCP PD（Prefix Delegation）に対応しています。

2.14 アライドテレシスマネージメントフレームワーク（AMF）

参照 「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク」

弊社スイッチ製品間で管理専用ネットワークを自動構成し、スイッチやネットワークの設定・運用を効率化するアライドテレシスマネージメントフレームワーク（AMF）をサポートしました。
AMF を利用するためには、AMF マスターとして動作する SwitchBlade x8100 システムが 1 台以上必要です。
AMF はデフォルトで有効となります。以前のバージョンからバージョンアップした場合も同様です。新規に AMF を利用する場合には、マスター、メンバーの初期設定が必要となります。

3 本バージョンで仕様変更された機能

ファームウェアバージョン **5.4.2A-0.1** から **5.4.3-0.1** へのバージョンアップにおいて、以下の機能が仕様変更されました。

3.1 リンクダウン / リンクアップ時のログレベル

参照 「コマンドリファレンス」/「運用・管理」/「ログ」

VLAN またはポートインターフェースでリンクダウン / リンクアップが起きた際に出力されるログのログレベルが「notice/5」になりました。

3.2 LDF の送出間隔

参照 「コマンドリファレンス」/「インターフェース」/「スイッチポート」

LDF の最小送出間隔を 5 秒から 1 秒に変更しました。

3.3 アクセスリスト

参照 「コマンドリファレンス」/「トラフィック制御」/「アクセスリスト」

show ipv6 access-list コマンドにて、IPv6 アクセスリスト名を指定して、特定のアクセスリストに登録されたエントリーのみを表示することができるようになりました。

4 本バージョンで修正された機能

ファームウェアバージョン **5.4.2A-0.1** から **5.4.3-0.1** へのバージョンアップにおいて、以下の項目が修正されました。

4.1 電源ユニットを 2 台装着して、両方とも電源を供給した状態で、片方の電源ユニットの電源供給を停止した後、電源供給を再開すると、show system environment コマンドの結果において、該当する電源ユニットの Status が Fault のままになることがありましたが、これを修正しました。

4.2 本来コンフィグモードで実行すべき do コマンドを非特権 EXEC モードや特権 EXEC モードで実行しようとしたとき、認識できないキーワードの先頭を指し示す「^」マークの位置が正しく表示されないことがありましたが、これを修正しました。

4.3 security-password forced-change コマンドで、パスワード有効期限が過ぎた次のログイン時にパスワード変更を求める表示が出るように設定しても、スタートアップコンフィグが存在しない場合、新パスワードの入力が拒否されログインできませんでしたが、これを修正しました。

4.4 TACACS+ サーバーを使用し、利用できるアカウントで筐体にログインした際、不要なメッセージが出力されましたが、これを修正しました。

4.5 RADIUS サーバーおよび TACACS+ サーバー機能を使用したユーザーのログインに失敗することがありましたが、これを修正しました。

4.6 email ログ送信時、メールヘッダーに From フィールド（送信元メールアドレス）を付けませんでしたが、これを修正しました。

4.7 VCS 構成で、マスター切り替えの際にメモリーリークが発生していましたが、これを修正しました。

4.8 4 台以上の VCS 構成の場合、起動時にまれに「### FIXME」というログメッセージが表示される場合がありましたが、これを修正しました。

4.9 トリガーを 250 個入力した場合、または 250 個のトリガーを含む起動時コンフィグファイルを指定して起動した場合に、本製品がリブートしていましたが、これを修正しました。

4.10 MIB-II の以下のオブジェクトの値を設定した場合に、本製品がリブートすることがありましたが、これを修正しました。

- currSoftSaveToFile
- nextBootPath
- backupPath
- bootCnfgPath
- backupCnfgPath

4.11 LDF 検出による検出時動作がいずれかのスイッチポートで発生すると、本体宛のパケットが破棄され、Ping に応答しなくなることがありましたが、これを修正しました。

4.12 SFP+ から送信側の光ケーブルのコネクターが抜けた場合、リンクアップとリンクダウンを繰り返し、対応するログメッセージを大量に生成していましたが、これを修正しました。

4.13 スタティックチャンネルグループ（手動設定のトランクグループ）とパケットストームプロテクションを併用する際、スタティックチャンネルグループに対してパケットストームプロテクションを設定すると正しく動作しませんでしたが、これを修正しました。

4.14 ゲスト VLAN に所属している Supplicant がスタティックチャンネルグループに所属している状態でスタティックチャンネルグループの設定を削除すると、認証の設定が消えているにもかかわらず、スタティックチャンネルグループに所属していたポートがゲスト VLAN に所属したままになっていましたが、これを修正しました。

4.15 VCS のバーチャル MAC アドレス機能を無効にして LACP が動作している場合、VCS マスター切り替えが発生すると、LACP チャンネルグループを無効に設定した際に関連プロセスが異常終了することがありましたが、これを修正しました。

4.16 LACP とポート認証を同一ポートで併用したとき、LACP ポートがリンクアップすると認証情報に対向機器の情報が載る場合がありましたが、これを修正しました。

4.17 本製品と Supplicant の間に EAP 透過スイッチをはさんだ状態で 802.1X 認証を使用すると、認証ポートを抜き差しした後すぐに行われる再認証が失敗していましたが、これを修正しました。

4.18 プロミスキャス / インターセプト Web 認証が有効な場合、IPv4 と IPv6 が有効な端末（Windows 7 など）から Web 認証画面にアクセスすることができませんでしたが、これを修正しました。

4.19 Web 認証サーバーにおいてセッションキープ機能が有効な場合、リダイレクトされる URL の末尾に不要な文字が付与されることがありましたが、これを修正しました。

4.20 IP サブネット VLAN において、設定済みの VLAN クラシファイアグループとルール番号を再度指定すると、重複して設定できていましたが、これを修正しました。

4.21 動作モードの設定（spanning-tree mode コマンド）が RSTP のとき、no spanning-tree force-version コマンドを使用して明示的なバージョン指定を削除することができませんでしたが、これを修正しました。

4.22 ECMP 環境において、一方のパスをソフトウェアルーティングで転送していましたが、これを修正しました。

4.23 ip address コマンドに label パラメーターを指定して IP アドレスにラベルを設定している状態で、ip address コマンドを no 形式で入力してラベルを削除する際、誤ったラベルを指定した場合、エラーメッセージが表示されずにラベルを削除できていましたが、誤ったラベルを入力した場合にエラーメッセージが表示されるように修正しました。

4.24 まれに、接続端末との ARP 解決に失敗し、その後 ARP テーブルへの登録ができないことがありましたが、これを修正しました。

4.25 ECMP 環境の IPv6 ネットワークでは、トラフィックが正しく分散されませんでしたが、これを修正しました。

4.26 show ip igmp interface コマンドの表示内容に Last member query count が 2 回出力されていましたが、これを修正しました。

4.27 VCS マスター切り替えが発生すると、手動設定のトランクグループ（スタティックチャンネルグループ）に設定されたポートで IGMP Query メッセージが転送されなくなることがありましたが、これを修正しました。

4.28 MLD Snooping の Report 抑制機能が有効な場合、代理送信する MLD メッセージの始点アドレスが「::」となり他の機器で破棄されていましたが、これを修正しました。

4.29 TCP/UDP のヘッダーを持たない、短い IPv6 マルチキャストパケットを複数受信すると、MLD Snooping 機能が正常に機能しなくなることがありましたが、これを修正しました。

4.30 TCP パケットに対するハードウェア IP アクセスリストをいずれかのポートに適用したまま設定を変更した場合、エラーメッセージが表示されず、設定も直ちに反映されませんでしたが、正しくエラーとして処理されるよう修正しました。

4.31 wrr-queue disable queues コマンドが正しく動作しませんでしたが、これを修正しました。

4.32 IP アドレスを割り当てていないインターフェースがある状態で DHCP サーバー機能を有効にした場合、DHCP サーバー機能が正しく動作しない場合がありましたが、これを修正しました。

4.33 default-router コマンドで、デフォルトゲートウェイアドレスとして正しくない値（255.255.255.255 など）を入力した際のエラーメッセージの内容が誤っていましたが、これを修正しました。

4.34 Ping ポーリング設定が 13 個以上存在していると、show counter ping-poll コマンドの結果が正しく表示されませんでしたが、これを修正しました。

4.35 複数の Ping ポーリングを設定していると、clear ping-poll all で Ping ポーリングのカウンターが初期化されませんでしたが、これを修正しました。

4.36 VCS 構成で boot system コマンドで起動ファームウェアを設定するとき、マスターに保存されているファームウェアをスレーブにコピーする場合、不要なログメッセージが表示されていましたが、これを修正しました。

4.37 VCS と NTP クライアント機能を併用している場合に、レジリエンシーリンクによるヘルスチェックに失敗する場合がありましたが、これを修正しました。

5 本バージョンでの制限事項

ファームウェアバージョン **5.4.3-0.1** には、以下の制限事項があります。

5.1 システム

参照「コマンドリファレンス」/「運用・管理」/「システム」

○ 次の通常起動時にロードされる通常用ファームウェアのイメージファイルが USB メモリー上にある状態で VCS のスタックメンバーに加入し、そのファームウェアが VCS マスターのものと異なると、次の緊急起動時にロードされるバックアップ用ファームウェアのイメージファイルが、USB メモリーではなくフラッシュメモリーにあるものとして指定されてしまいます。

○ ダイナミックコンフィグ上で、no ip name-server、no ip domain-lookup を設定しても DNS 問い合わせ機能が無効になりません。

○ 本製品は SD カードには対応していませんが、USB オートブート時に、SD カードに関するエラーメッセージがログに出力されます。これは表示のみの問題であり、動作には影響しません。
- daemon.err awplus automount[2577]:

5.2 コマンドラインインターフェース（CLI）

参照 「コマンドリファレンス」/「運用・管理」/「コマンドラインインターフェース」

edit コマンドを使用すると、コンソールターミナルのサイズが自動で変更されてしまいます。

5.3 ファイル操作

参照 「コマンドリファレンス」/「運用・管理」/「ファイル操作」

○ ZMODEM を使用して、ファイルサイズ 3 MByte 以上のファイルを転送すると、リブートすることがあります。

○ USB メモリーに空き容量がない状態で、create autoboot コマンドを実行するとエラーメッセージが表示され、その後別の USB メモリーを使用しようとすると、正しくディレクトリーが読み取れません。エラーメッセージ出力後に別の USB メモリーを使う際は、一度本体を再起動してから使用してください。同一の USB メモリーを使用するには問題ありません。

○ cd コマンドにて USB メモリーを利用中、USB メモリーを抜くと、その後再度 USB メモリーを挿しても認識されません。USB メモリーを抜く前には必ず、cd flash で USB メモリーの利用を中止してください。

○ USB メモリーを取り外した時のメッセージが Enter キーを入力するまで表示されません。

5.4 ユーザー認証

参照 「コマンドリファレンス」/「運用・管理」/「ユーザー認証」

○ アクセスが許可されていないホスト / ユーザーから SSH でログインしようとした場合、コンソール上にデバッグメッセージが表示されます。

○ tacacs-server timeout コマンドで設定できるタイムアウト値の最大は 190 秒です。

○ ユーザー認証に TACACS+ を使用するとき、同時に使用できる仮想端末ポート（VTY）の数は 20 までとなります。また内部のユーザー認証データベースを使用するときは、同時に使用できる仮想端末ポート（VTY）の数は 33 までとなります。

○ TACACS+ 認証を使用して VCS マスターにログイン後、他のスタックメンバーにリモートログインしている最中に、ほかの TACACS+ セッションが同じユーザー名、パスワードでログインすると、以下のメッセージが出力されます。
- You don't exist, go away!

5.5 RADIUS クライアント

参照「コマンドリファレンス」/「運用・管理」/「RADIUS クライアント」

ローカル RADIUS サーバーに登録していない RADIUS クライアント（NAS）から、RADIUS Access-Request パケットを受信した場合、show radius local-server statistics コマンドで表示される Unknown NAS のカウンターがカウントアップしません。

5.6 RADIUS サーバー

参照「コマンドリファレンス」/「運用・管理」/「RADIUS サーバー」

○ USB メモリーを利用してローカル CA の証明書をダウンロードする際、USB メモリーにすでに同じ名前のローカル CA の証明書が入っていた場合、Overwrite usb:/rootca.cer? (y/n) と確認のメッセージが表示されますが、Y も N も入力できず、上書きできません。USB メモリーに入っているファイルを削除するか、ファイル名を 変更してダウンロードを行ってください。

○ server auth-port コマンドによりローカル RADIUS サーバーの認証用 UDP ポート番号を 63998 以上に設定しようとすると、関連プロセスが再起動するログが出力されます。また、上記の UDP ポート番号を使用してポート認証を行うことができません。

5.7 ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

○ 保存するメッセージの最大量が log size コマンドで設定した値と異なります。

○ MSTP 有効時、多数のインターフェースが同時にアップまたはダウンし、ログメッセージが大量に発生した場合、すべてのログメッセージが Syslog サーバーに転送されない場合があります。

○ ターミナルモニターを有効にした後、VCS のバックアップメンバーにリモートログインを行いながら USB メモリーを抜き差しすると、ターミナルモニターのログが正しく表示されません。

○ no log buffered コマンドを入力してランタイムメモリー（RAM）へのログ出力を一度無効にし、default log buffered コマンドを実行すると、ログが出力されなくなります。

○ 以下のログがコンソールに表示されないことがあります。
- Configuration update completed for portxxx
- Member x (xxxx.xxxx.xxxx) has become the Active Master

5.8 トリガー

参照「コマンドリファレンス」/「運用・管理」/「トリガー」

トリガー設定時、script コマンドで指定したスクリプトファイルが存在しない場合、コンソールに出力されるメッセージ内のスクリプトファイルのパスが誤っています。

誤：

% Script /flash/script-3.scp does not exist. Please ensure it is created before

正：

% Script flash:/script-3.scp does not exist. Please ensure it is created before

また、スクリプトファイルが存在しないにもかかわらず前述のコマンドは入力できてしまうため、コンフィグに反映され、show trigger コマンドのスクリプト情報にもこのスクリプトファイルが表示されます。

5.9 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ LACP を使用しトランクグループを作成した際、対向機器の SNMP マネージャーで linkDown トラップを受信できない場合があります。送信先ホストの設定をする際、通知メッセージの形式で informs を指定すると informs パケットが受信できます。

○ VCS 構成のシャーシに GetNext Request を送信すると、SNMP が「no such object」と応答することがあります。

○ SNMP MIB で、ifHCInUcastPkts と ifHCOutUcastPkts の値が正しくありません。それぞれ、ユニキャストパケットの受信数と送信数を示すはずですが、ブロードキャスト / マルチキャストパケットもカウントされてしまいます。

○ snmp-server enable trap コマンドは、省略せずに入力してください。省略した場合、実行できない、または、コンソールの表示が乱れることがあります。

○ 一定以上の文字数の名前を持つファイルが保存された状態で、SNMP MIB の atFilev2FileViewerName を get しようとすると、関連プロセスが異常終了し、本製品がリブートします。

5.10 sFlow

参照「コマンドリファレンス」/「運用・管理」/「sFlow」

○ sflow collector コマンドで sflow の UDP ポートを設定したとき、コンフィグに反映されず、保存、再起動で初期設定に戻ってしまいます。再起動した場合は、再度設定してください。SNMP マネージャーから設定した場合も同様です。

○ sFlow が有効なインターフェースで VLAN タグがついたパケットを受信したとき、ingress 方向のサンプリング情報に VLAN タグ情報が付与されません。

○ sFlow MIB の sFlowFsReceiver と sFlowCpReceiver の値を変更後、初期値に戻すためには sFlow を無効にする必要があります。

5.11 NTP

参照「コマンドリファレンス」/「運用・管理」/「NTP」

○ 実際には NTP サーバーと時刻同期が取れていない状態でも、show ntp associations コマンド上では同期済みと表示される場合があります。

○ NTP を使用していると、以下のログが出力されますが、動作には問題ありません。

- frequency error 501 PPM exceeds tolerance 500 PPM

○ NTP を設定していないときでも、NTP カウンターがカウントアップします。

○ すでに NTP サーバーが設定されている状態で、別のサーバーに設定を変更した場合、一度設定を削除した後、新規に設定を追加してください。削除せずに変更した場合、正しく同期しない場合があります。

○ 初期設定時など、NTP を設定していない状態で show ntp status コマンドを入力すると、NTP サーバーと同期していることを示す以下のようなメッセージが表示されます。
- Clock is synchronized, stratum 0, actual frequency is 0.000PPM, presicion is 2

○ show ntp association detail コマンドの org time および xmt time の表示が、NTP による同期の有無にかかわらず、「06:28:16.000 UTC Thu Feb 7 2036」を示します。これは表示だけの問題で、システムの時計の動作には影響しません。

○ NTPv4 を使用している場合、ntp master コマンドによる NTP 階層レベル（Stratum）の設定と NTP サーバーによる時刻の取得を併用すると、NTP サーバーによって自動決定される階層レベルが優先されます。

○ NTP ピアまたは NTP サーバーのアドレスにドメイン名を指定した場合、コンソールの反応が数分の間停止した り、ドメイン名が正常に解決され、時刻を同期できているにもかかわらず、「Warning: Host xxx cannot be resolved」メッセージが表示されたりすることがあります。

5.12 端末設定

参照「コマンドリファレンス」/「運用・管理」/「端末設定」

○ clear line console コマンドを実行すると、他の VCS メンバー上のコンソールで接続しているユーザーのセッションも切断されます。

○ コンソールターミナルおよび仮想端末における 1 画面当たり表示行数は、実際のコンソールターミナルや仮想端末に表示できる行数より小さい値に設定してください。

5.13 Telnet

参照「コマンドリファレンス」/「運用・管理」/「Telnet」

本製品から他の機器に Telnet で接続しているとき、次のようなメッセージが表示されます。
- No entry for terminal type "network";
- using vt100 terminal settings.

5.14 インターフェース

参照「コマンドリファレンス」/「インターフェース」

○ show interface コマンドで表示される dropped カウンターがカウントされません。show platform port counters コマンドの ifInDiscards カウンターで確認してください。

○ IPv6 アドレスを持つインターフェースに show interface コマンドを入力した際の結果に、実際のホップリミットの値が表示されません。

○ 1 つのインターフェースに設定可能な IPv6 アドレスは 16 アドレスまでです。

5.15 ポートセキュリティー

参照 「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ ジャンボフレームとポートセキュリティーは併用できません。

○ ポートセキュリティーによって学習された MAC アドレスをエージアウトしないよう設定し、ポートセキュリティーの不正パケット受信時の動作を指定している場合、ポートセキュリティーを無効にしてもスタティック MAC アドレスがコンフィグに残ったままになります。コンフィグに残ってしまったスタティック MAC アドレスは、no mac address-table static または、clear mac address-table コマンドで削除してください。

○ ポートセキュリティーにおいて、不正パケット受信時の動作を shutdown に設定している状態で、ポートセ キュリティーを無効にすると、ログが正しく出力されず、show interface status コマンドでインターフェースのステータスが正しく表示されません。shutdown コマンドでインターフェースを無効にし、その後有効にする ことで正しく表示されます。

5.16 ループガード

参照 「コマンドリファレンス」/「インターフェース」/「スイッチポート」

○ QoS と LDF 検出を同一ポートで併用した場合、LDF パケットを受信してもループを検出できません。

○ LACP と LDF 検出は併用できません。

○ LDF 検出機能により、ループを検出した VLAN のポートが無効化されている場合、switchport enable vlan コマンドを VID を指定せずに実行しても、無効化されている VLAN のポートは有効になりません。LDF 検出機能により無効化されている VLAN のポートを有効にするには、switchport enable vlan コマンドを VID を指定して実行してください。

○ LDF 送信間隔(loop-protection コマンドの ldf-interval パラメーター)を最小値の 1 秒に設定する場合、ループ検出時の動作持続時間(loop-protection timeout コマンド)は 2 秒以上に設定してください(初期値は 7 秒)。

○ 本来、LDF 機能はアクセスリストのエントリーに空きがない場合には使用できませんが、アクセスリストのエン トリーに空きがない場合でも、loop-protection loop-detect コマンドを 1 回入力し、エラーメッセージが表示された後に、再度同じコマンドを入力すると、コマンドが実行されてしまいます。
また、loop-protection loop-detect コマンドを 1 回入力し、エラーメッセージが表示された後に、当該のポートからアクセスリストのエントリーを削除すると、アクセスリストの登録数と最大数が正しく表示されなくなります。

○ MAC アドレススラッシング検出時の動作に learn-disable アクションを設定しているとき、MAC アドレススラッシング検出後、MAC アドレスの学習が停止されないことがあります。

○ MAC アドレススラッシングプロテクション設定時、ループを検出したすべてのポートが、設定した動作を行います。

5.17 リンクアグリゲーション（IEEE 802.3ad）

参照 「コマンドリファレンス」/「インターフェース」/「リンクアグリゲーション」

○ ポート認証と LACP を同一ポートで併用することはできません。認証ポートではスタティックチャンネルグループ（手動設定のトランクグループ）を設定するようにしてください。

○ スタティックチャンネルグループの対向機器の先に SNMP マネージャーが接続されている場合、スタティックチャンネルグループのメンバーポートをリンクアップした際、対向機器のリンクアップトラップが SNMP マネージャーに送信されないことがあります。

○ トランクグループ（saX, poX）に対して egress-rate-limit コマンドを実行した場合、送信レート上限値はトランクグループ全体に対してではなく、メンバーポート 単位で適用されます。またこのとき、ランニングコンフィグ上でもトランクグループではなくメンバーポートに対する設定に変換されます（CLI からメンバー ポートに対して同コマンドを実行するとエラーになりますが、スタートアップコンフィグから読み込んだときはエラーになりません)。

○ スタティックチャンネルグループ（手動設定のトランクグループ）において、shutdown コマンドによって無効にしていたポートに対して no shutdown コマンドを入力しても、ポートが有効にならないことがあります。
この場合は、再度 shutdown コマンド、no shutdown コマンドを入力してください。

○ スタティックチャンネルグループのインターフェースを shutdown コマンドにより無効に設定した後、リンクアップしているポートをそのスタティックチャンネルグループに追加すると、該当するインターフェースが再び有効になります。

○ LACP ポート上にエンハンストプライベート VLAN のセカンダリーポートを設定することは未サポートとなります。

5.18 ポート認証

参照 「コマンドリファレンス」/「インターフェース」/「ポート認証」

○ EAP 透過機能で forward（受信した EAPOL パケットを VLAN に関係なくすべてのポートに転送する）に設定した場合、ポートミラーリングのソースポートからコピーされた EAPOL パケットとは別にミラーポートへ EAPOL パケットが転送されます。

○ Web 認証サーバーのインターセプトモードとセッションキープ機能を併用すると、セッションキープ機能が働かない場合があります。

○ dot1 control-direction コマンドの both オプションは未サポートです。

○ Supplicant の再認証間隔（reAuthPeriod）の初期値は 3600 秒ですが、2 回目の再送間 隔は約 1800 秒と前回の再送間隔の約半分になります。一定間隔で再送する場合は、auth timeout reauth-period コマンドで初期値以外の値を設定してください。

○ VCS とリンクアグリゲーション併用時、トランクポートで認証を行った後、Supplicant 宛てのパケットを VCS のスレーブで受信すると不必要なログメッセージが出力されます。

○ ローミング認証有効時、同時に多数の Supplicant のポート移動を行うと、再認証が発生する場合があります。

○ スタティックチャンネルグループ内にゲスト VLAN に所属している Supplicant がいると、そのトラン クポートのコンフィグに switchport access vlan の設定が追加されてしまいます。チャンネルグループを削除しても switchport access vlan の設定は残るので、先に switchport access vlan の設定を削除してからチャンネルグループを削除してください。

○ 802.1X 認証の Supplicant がログオフしても、ステータスが Connecting になりません。

○ プロミスキャス / インターセプト Web 認証使用時、認証成功後にリダイレクトされた Web ページの表示に失敗することがあります。その場合は Web ページを再読み込みしてください。

○ 64 文字のユーザー名でポート認証を行うと、認証に失敗します。

○ 802.1X 認証において、Auth-fail VLAN の設定を初期値のままにしていると Auth-fail VLAN へ移行できない場合があります。
dot1x max-reauth-req コマンドで設定する EAPOL パケットの最大再送回数を dot1x max-auth-fail コマンドで設定する Supplicant の最大ログイン試行回数以上に設定してください。

○ Web 認証において、一度プロミスキャスモードに設定すると、その後インターセプトモードに変更しても、プロミスキャスモード設定時と同様に、動作します。
インターセプトモードに設定を変更後、コンフィグを保存し、再起動した場合は、インターセプトモードとして動作します。

○ 802.1X 認証において、認証を 3 台以上の RADIUS サーバーにて行う場合、はじめの 2 台の RADIUS サーバーにて認証に失敗した際、Authenticator から 3 台目の RADIUS サーバーに Access-Request が送信されません。

○ 認証済みポートが認証を解除された場合、マルチキャストトラフィックが該当のポートにも転送され続ける場合があります。

5.19 バーチャル LAN

参照「コマンドリファレンス」/「L2 スイッチング」/「バーチャル LAN」

○ vlan コマンドは数値とカンマ、ハイフンだけを受け付ける仕様ですが、指定値にこれら以外の文字が含まれて いてもエラーになりません。このとき、意図した VLAN が作成されなかったり（例：「10,20」のつもりで「10.20」と誤入力すると「10」しか作 成されない）、意図したのとは異なる VLAN が作成されたりする（例：「1001」のつもりで「100q」と誤入力すると「100」が作成される）場合が ありますのでご注意ください。

○ 大量に VLAN を作成後、switchport trunk allowed vlan コマンドを except オプション付きで指定しトランクポートの設定を行うと、再起動することがあります。
switchport trunk allowed vlan コマンドを except オプション付きで指定するときには、VLAN 数を 700 以内にしてください。または、except オプションではなく、add または、all オプションを設定してください。

○ プライベート VLAN からプライマリー VLAN を削除する場合は、事前にプライマリー VLAN、セカンダリー VLAN ともに、プライベート VLAN の関連付けを解除してください。その後、プライマリー VLAN のみを削除、再作成し、改めてプライベート VLAN と プライマリー VLAN、セカンダリー VLAN の関連付けを行ってください。

○ エンハンストプライベート VLAN を設定したポートからプライベート VLAN 用ポートとしての設定を削除すると、該当のポートでパケットが転送できなくなります。プライベート VLAN 用ポートとしての設定を削除した後は、本製品を再起動してください。

○ プライベート VLAN のプロミスキャスポートに手動設定のトランクグループ（スタティックチャンネルグループ）を設定した場合、再起動後、ホストポートへパケットが転送されません。
再起動後、プロミスキャスポートの設定を再入力すると、パケットが正常に転送されるようになります。

5.20 GVRP

参照「コマンドリファレンス」/「L2 スイッチング」/「GVRP」

学習する VLAN 情報が多い場合、GVRP を設定しているポートをダウンさせ、その後すぐにアップさせると、正常に VLAN 情報が学習できなくなります。GVRP を利用する際の最大 VLAN 数は、100 です。

5.21 スパニングツリープロトコル

参照「コマンドリファレンス」/「L2 スイッチング」/「スパニングツリープロトコル」

チャンネルグループを作成後に MSTP を有効にすると、FDB に学習した MAC アドレスがケーブルがリンクダウンしてもクリアされません。チャンネルグループを作成する前に MSTP を有効にしてください。

5.22 イーサネットリングプロテクション（EPSR）

参照 「コマンドリファレンス」/「L2 スイッチング」/「イーサネットリングプロテクション」

○ EPSR の経路切り替えが発生した際、EPSR ポートから送信された一部のトラップが SNMP マネージャーに到達できない場合があります。

○ EPSR と GVRP の併用は未サポートになります。

5.23 DHCP Snooping

参照 「コマンドリファレンス」/「L2 スイッチング」/「DHCP Snooping」

snmp-server enable trap コマンドで DHCP Snooping 関連のトラップを有効に設定しているとき、ip dhcp snooping violation コマンドでトラップを設定しようとすると、「SNMP trap for DHCP Snooping is disabled」というメッセージが表示され、トラップの設定が有効になりません。トラップを設定する場合は、ip dhcp snooping violation コマンド、snmp-server enable trap コマンドの順に入力してください。また、上記のエラーメッセージが表示された場合は、再度 snmp-server enable trap コマンドを入力することで、トラップの設定が有効になります。

5.24 IP ルーティング

参照 「コマンドリファレンス」/「IP ルーティング」

ループバックインターフェースに IP アドレスを設定した時、ループバックインターフェース宛のルートエントリーがハードウェアテーブルに登録されません。

5.25 IPv6 ルーティング

参照 「コマンドリファレンス」/「IPv6 ルーティング」

○ IPv6 アドレスを設定する際、不正なインターフェース ID が指定されてもエラーになりません。

○ 6to4 のトンネリングが確立している状態で DSCP 値をダイナミックに変更すると、その後トンネリングの確立に失敗します。DSCP 値を変更する場合は、変更後の設定を保存後、機器を再起動してください。

○ 自身の IPv6 アドレス宛に ping を実行するとエラーメッセージが表示されます。

5.26 IPv6 インターフェース

参照 「コマンドリファレンス」/「IPv6 ルーティング」/「IPv6 インターフェース」

6to4 トンネリングパケットの外側ヘッダーに TTL 値を指定すると、トラフィックが流れなくなります。

5.27 IGMP

参照 「コマンドリファレンス」/「IP マルチキャスト」/「IGMP」

○ ip igmp static-group コマンドで source パラメーターを指定しても、指定した送信元 IP アドレス以外からのマルチキャストパケットも指定したポートにだけ送信してしまいます。

○ show ip igmp groups コマンドの表示結果に、IGMP を有効に設定していない VLAN が表示されることがあります。これは show ip igmp groups コマンドの表示だけの問題であり、動作に影響はありません。

○ IGMP プロキシーにおいて、下流インターフェースに指定している VLAN を無効にしても、上流インターフェースにグループ情報が残り続けます。

○ マルチキャストグループをスタティックに登録した後、登録したインターフェースにスタティックに登録してあるものと同じマルチキャストグループの参加、離脱が発生すると、マルチキャストグループがコンフィグから削除しても消せなくなります。
この場合は、マルチキャストグループにメンバーが参加した状態で ip igmp static-group コマンドを no 形式で実行するか、IGMP 機能を一旦無効にし、再度有効にすると、マルチキャストグループは正常に削除されます。

5.28 IGMP Snooping

参照 「コマンドリファレンス」/「IP マルチキャスト」/「IGMP Snooping」

○ スタティックに設定されたルーターポートで IGMP Query メッセージを受信すると、受信後 260 秒後に登録が解除されます。

○ IGMP Snooping の Report 抑制機能が無効の場合（no ip igmp snooping report-suppression）、Leave メッセージを受信すると、ルーターポートへ 2 パケット転送されます。

○ IGMP Snooping が有効な状態で、一旦無効にし、再度有効にした場合、その後に受信する IGMP Report を全ポートにフラッディングします。
IGMP Snooping を再度有効にした後、clear ip igmp group コマンドを実行して全てのエントリーを消去することで回避できます。

○ グローバルコンフィグモードの ip igmp snooping コマンド、インターフェースモードの ip igmp snooping コマンドのどちらか一方のみが実行されている状態では、不要なパケットが複製され出力されます。

○ IGMP Snooping の設定を無効で起動した場合、有効に変更しても、IGMP パケットが正しく転送されません。IGMP Snooping を無効から有効に設定変更した場合は、設定を保存し再起動してください。

5.29 MLD Snooping

参照 「コマンドリファレンス」/「IPv6 マルチキャスト」/「MLD Snooping」

○ IPv6 マルチキャストパケットの受信中に MLD Snooping を無効から有効に変更すると、MLD Snooping が有効になりません。MLD Snooping を無効から有効に変更するときは、IPv6 マルチキャストの通信が行われていない状態で実施してください。

○ MLD Snooping の Report 抑制機能が有効なとき（初期設定は有効）、ルーターポートで受信した MLDv1 Report または Done メッセージを受信ポートから再送出してしまいます。これを回避するには、「no ipv6 mld snooping report-suppression」で Report 抑制機能を無効化してください。

○ グローバルコンフィグモードの ipv6 mld snooping コマンド、インターフェースモードの ipv6 mld snooping コマンドのどちらか一方のみが実行されている状態では、不要なパケットが複製され出力されます。

○ MLD Snooping の設定を無効で起動した場合、有効に変更しても、MLD パケットが正しく転送されません。MLD Snooping を無効から有効に設定変更した場合は、設定を保存し再起動してください。

5.30 アクセスリスト

参照 「コマンドリファレンス」/「トラフィック制御」/「アクセスリスト」

ntp access-group コマンドによって NTP サービスに対するアクセス制御の設定を行う場合、ホストを許可（permit）する形式で標準 IP アクセ スリストを作成していると、エントリーにマッチするホストのみでなく、マッチしないホストも時刻の同期を行うことができてしまいます。
標準 IP アクセスリストを作成する際、許可するホストを指定したあとに、すべてを拒否（deny any）するエントリーを追加してください。

5.31 ハードウェアパケットフィルター

参照 「コマンドリファレンス」/「トラフィック制御」/「ハードウェアパケットフィルター」

○ IGMP パケットはハードウェアパケットフィルターでフィルタリングできません。

○ トランクポート上で OSPF の Hello パケットをフィルタリングできません。

5.32 Quality of Service

参照 「コマンドリファレンス」/「トラフィック制御」/「Quality of Service」

○ QoS の match eth-format protocol コマンドで AppleTalk パケットを制御できません。

○ match dscp コマンドの設定を削除する際、no match dscp と入力するとエラーとなります。
no match ip-dscp コマンドを入力することで、設定を削除できます。

○ wrr-queue disable queue コマンドの設定を削除する場合、no mls qos コマンドよりも先に no wrr-queue disable queue コマンドを実行してください。

○ QoS の送信スケジューリング方式（PQ、WRR）が混在するポートを手動設定のトランクグループ（スタ ティックチャンネルグループ）に設定した場合、ポート間の送信スケジュールが正しく同期されません。トランクグループを設定した場合は、個々のポートに同 じ送信スケジュール方式を設定しなおしてください。

5.33 攻撃検出

参照「コマンドリファレンス」/「トラフィック制御」/「攻撃検出」

dos teardrop コマンドは未サポートです。

5.34 DNS リレー

参照「コマンドリファレンス」/「IP 付加機能」/「DNS リレー」

DNS のキャッシュサイズまたはタイムアウトの設定を変更すると、IPv6 DNS キャッシュエントリーが削除されます。

5.35 DHCP サーバー

参照「コマンドリファレンス」/「IP 付加機能」/「DHCP サーバー」

DHCP サーバー機能において、使用期限の切れた IP アドレスがデータベースから削除されません。
なお、IP アドレスを割り当てる際には、IP アドレスが使用中かどうか確認してからクライアントに割り当てているため、動作に影響はありません。

5.36 Ping ポーリング

参照「コマンドリファレンス」/「IP 付加機能」/「Ping ポーリング」

Ping ポーリング機能を一旦無効化してから再度有効化すると、プロセス終了を示す以下のようなログが表示されますが、動作に問題はありません。

- init: network/ping-poll main process (13750) killed by HUP signal

5.37 アライドテレシスマネージメントフレームワーク（AMF）

参照「コマンドリファレンス」/「アライドテレシスマネージメントフレームワーク」

○ AMF クロスリンク、EPSR、VCS を使用した構成で、VCS メンバーがダウンし、復旧した際、復旧した VCS メンバーに接続されている AMF ノードが認識されません。
EPSR リング内では、AMF Node Depth 値が異なる AMF ノード同士は AMF リンクで接続してください。

○ VCS 構成において、スタックリンクに障害が発生し VCS メンバーが Disabled Master 状態になると、スタックリンクとレジリエンシーリンク以外のポートは無効化されますが、EPSR を併用している場合、show atmf nodes コマンドの結果には、Disabled Master 状態となり無効化されたポートに接続された AMF ノードが表示されてしまいます。

EPSR リング内では、AMF マスターからの距離（ホップ数）の異なる AMF ノード同士は、AMF クロスリンクではなく AMF リンクで接続してください。

5.38 バーチャルシャーシスタック（VCS）

参照「コマンドリファレンス」/「バーチャルシャーシスタック」

○ VCS バックアップメンバーが再加入中にコンフィグを変更すると、再加入したバックアップメンバーにコンフィグが反映されないことがあります。バックアップメンバーが加入中に設定の変更はしないでください。

○ まれに VCS マスター切り替え後の新マスターが、設定されているプライオリティー値に従わずに選定されることがあります。

○ VCS スレーブを交換する際、マスターとスタックケーブルで接続して電源をオンにした後、通常、スタック ID を変更し、AMF を有効に設定するため、2 回の再起動が必要になりますが、AMF ネットワークに所属後、コンフィグの同期に時間がかかり、コンフィグの同 期後に以下のようなエラーメッセージが表示され、もう一度再起動を要求されます。
- Post startup check found the following errors:
- Processes not ready:
- authd bgpd epsrd irdpd lacpd lldpd mstpd ospf6d ospfd pdmd pim6d pimd ripd ripngd rmond sflowd vrrpd
- Timed out after 300 seconds
- Bootup failed, rebooting in 3 seconds.
- Do you wish to cancel the reboot? (y) :

○ LDF が検出され link-down アクションが実行されている間にループを解消し、VCS マスター切り替えが発生すると、LDF 検出時アクションが実行されたポートが設定時間経過後も復旧しません。
該当のポートにて shutdown コマンドを no 形式で実行すると、リンクが復旧します。

○ VCS と EPSR を併用する場合、reboot rolling コマンドを実行した際に約 1 分程度の通信断が発生する場合があります。

6 マニュアルの補足・誤記訂正

最新マニュアル（取扱説明書、コマンドリファレンス、VCS 設定 / 運用マニュアル）の補足事項および誤記訂正です。

6.1 AT-x510-28GTX/AT-x510-52GTX の定格入力電流

参照「取扱説明書」（Rev.A）64 ページ

取扱説明書（Rev.A）64 ページ「本製品の仕様」の表において、AT-x510-28GTX と AT-x510-52GTX の定格入力電流の記載に誤りがありましたので、下記のとおり訂正いたします。

誤：

―	*AT-x510-28GTX*	*AT-x510-52GTX*
電源部		
定格入力電流	1.1A	1.1A
最大入力電流（実測値）	0.97A	0.96A
平均消費電力	41W（最大 52W）※4	69W（最大 86W）※4
平均発熱量	150kJ/h（最大 190kJ/h）※4	240kJ/h（最大 310kJ/h）※4

※4 AT-SP10LR × 4 個 使用時

正：

―	*AT-x510-28GTX*	*AT-x510-52GTX*
電源部		
定格入力電流 （AC 電源× 1 個）	1.0A	1.0A
AC 電源× 1 個 使用時		
最大入力電流（実測値）	0.97A	0.96A
平均消費電力	41W（最大 52W）※4	69W（最大 86W）※4
平均発熱量	150kJ/h（最大 190kJ/h）※4	240kJ/h（最大 310kJ/h）※4
AC 電源× 2 個 使用時		
最大入力電流（実測値）	0.97A	0.96A
平均消費電力	41W（最大 52W）※4	69W（最大 86W）※4
平均発熱量	150kJ/h（最大 190kJ/h）※4	240kJ/h（最大 310kJ/h）※4

※4 AT-SP10LR × 4 個 使用時

6.2 NTP

参照 「コマンドリファレンス」/「運用・管理」/「NTP」

NTP の認証が有効な NTP クライアントとして動作している場合でも、NTP の認証が有効でない NTP サーバーと時刻同期ができてしまいます。

6.3 スパニングツリープロトコル

参照 「コマンドリファレンス」/「L2 スイッチング」/「スパニングツリープロトコル」

片方向通信中に STP でトポロジーチェンジが発生した場合、宛て先 MAC アドレスがエージアウトしない場合があります。片方向通信のみの環境では、RSTP または MSTP を使用してください。

6.4 フォワーディングデータベース

参照 「コマンドリファレンス」/「L2 スイッチング」/「フォワーディングデータベース」

登録されている MAC アドレス宛てへ通信を転送している場合、エージングタイム経過後も該当アドレスが MAC テーブルから削除されません。

7 サポートリミット一覧

パフォーマンス	
VLAN 登録数	単体：4094 VCS：2000 ※ 1
MAC アドレス（FDB）登録数	単体：16K VCS：4K ※ 2
IPv4 ホスト（ARP）登録数	単体：2K VCS：768 ※ 3
IPv4 ルート登録数	1K ※ 4
リンクアグリゲーション	
グループ数（筐体あたり）	128 ※ 5
ポート数（グループあたり）	8
ハードウェアパケットフィルター	
登録数	237 ※ 6 ※ 7
認証端末数	
認証端末数（ポートあたり）	1K
認証端末数（装置あたり）	1K
マルチプルダイナミック VLAN（ポートあたり）	1K
マルチプルダイナミック VLAN（装置あたり）	1K
ローカル RADIUS サーバー	
ユーザー登録数	100
RADIUS クライアント（NAS）登録数	24
その他	
VRF-Lite インターフェース数	-
IPv4 マルチキャストルーティングインターフェース数	-

※　表中では、K=1024
※ 1 VCS 構成時、VCS グループに設定する VLAN の数は 2000 個までをサポートします。
※ 2 VCS 構成時、フォワーディングデータベース（FDB）のエントリー数は 4K 個までサポートします。
※ 3 VCS 構成時、IPv4 ホスト登録数（ARP エントリー数）は最大で 768 個までサポートします。
※ 4 インターフェース経路およびスタティック経路を含めた登録数です。
※ 5 スタティックチャンネルグループは 96 グループ、LACP は 32 グループ設定可能。合わせて 128 グループをサポートします。
※ 6 アクセスリストのエントリー数を示します。
※ 7 エントリーの消費量はルール数やポート数に依存します。

8 未サポート機能（コマンド）

最新のコマンドリファレンス、VCS 設定 / 運用マニュアルに記載されていない機能、コマンドはサポート対象外ですので、あらかじめご了承ください。最新マニュアルの入手先については、次節「最新マニュアルについて」をご覧ください。

9 最新マニュアルについて

最新の取扱説明書「CentreCOM x510 シリーズ 取扱説明書」(613-001684 Rev.A)、コマンドリファレンス「CentreCOM x510 シリーズ コマンドリファレンス」(613-001763 Rev.A)、「CentreCOM x510 シリーズ VCS 設定 / 運用マニュアル」(613-001766 Rev.A)は弊社ホームページに掲載されています。

本リリースノートは、これらの最新マニュアルに対応した内容になっていますので、お手持ちのマニュアルが上記のものでない場合は、弊社 Web ページで最新の情報をご覧ください。

http://www.allied-telesis.co.jp/